Cryptool

1. Δημιουργία κειμένου.
2. Κλασική κρυπτογραφία:
    a. Κρυπτογράφηση – αποκρυπτογράφηση – κρυπταναλυση με Caesar
    b. Κρυπτογράφηση – αποκρυπτογράφηση με αλγόριθμο XOR
    c. Κρυπτογράφηση – αποκρυπτογράφηση με αλγόριθμο Vernam Cipher (one-time pad)
3. Συμμετρική κρυπτογραφία:
    a. Κρυπτογράφηση – αποκρυπτογράφηση με αλγόριθμο RC2
        i. Κλειδί 16 bit – κρυπτανάλυση
        ii. Κλειδί 40 bit - κρυπτανάλυση
        iii. Κλειδί 128 bit- κρυπτανάλυση
    b. Κρυπτογράφηση – αποκρυπτογράφηση με αλγόριθμο DES (ECB mode)
    c. Επίδειξη DES
    d. Κρυπτογράφηση – αποκρυπτογράφηση με αλγόριθμο AES – self extracting
    e. Επίδειξη AES
4. Συναρτήσεις κατακερματισμού
    a. Δημιουργία σύνοψης αρχείου με συνάρτηση κατακερματισμού MD5
    b. Δημιουργία σύνοψης αρχείου με συνάρτηση κατακερματισμού SHA
    c. Παράδειγμα σύγκρουσης με test message
5. Ασύμμετρη κρυπτογραφία:
    a. Δημιουργία κλειδιών RSA
    b. Εμφάνιση πληροφοριών των κλειδιών
    c. Κρυπτογράφηση – αποκρυπτογράφηση με αλγόριθμο RSA
        i. Χρήση μεγάλου αρχείου και σύγκριση κρυπτογράφησης – αποκρυπτογράφησης AES και RSA. Εμφάνιση χρόνου.
    d. Επίδειξη RSA
    e. Επίδειξη Diffie-Hellman με μικρούς αριθμούς (π.χ. p=13, g=3, a=2, b=3)
    f. Ψηφιακή υπογραφή
        i. Δημιουργία υπογραφής με RSA
        ii. Επίθεση σε ψηφιακή υπογραφή
6. Κρυπτανάλυση:
    a. Επιλογή παραμέτρων (πρώτων αριθμών) RSA για διάφορες τιμές και δομική επιθέσεων παραγοντοποίησης
7. Υβριδική κρυπτογραφία:
    a. Κρυπτογράφηση – αποκρυπτογράφηση (μεγάλου αρχείου) με υβριδική κρυπτογραφία. (εμφάνιση χρόνου)

GNU PGP

1) Εγκατάσταση GPG4Win (μαζί με το GPA)
2) **GPA** (Gnu Privacy Assistant)
    a. Keys → New Key (Δημιουργία ζεύγους κλειδιών))
    b. Keys → Set Owner Trust
    c. Keys → Sign Keys (Υπογραφή του δικού μας κλειδιού)
    d. Keys → Set Owner Trust
    e. Keys → Import / Export / Backup keys
    f. Windows → File Manager (Encrypt, sign, decrypt, verify a file)
    g. Windows → Clipboard (edit, encrypt, decrypt)
    h. Server → Send / retrieve keys
3) Kleopatra (management of OpenPGP, X.509 certificates)